Wydanie z dnia: czwartek, 3. marzec 2022»Kadry i płace

Zweryfikujcie w firmie listy dostępu do danych – w tym z PUE ZUS

Odchodzącego pracownika bądź np. biuro rachunkowe, z którego usług przyszło nam zrezygnować, należy odsunąć od danych osobowych odpowiednio wcześniej. Nie ma znaczenia, czy i w jakiej skali ktoś zrobi z nich użytek. Takie wnioski płyną z niedawnej decyzji UODO i dotyczą logowania się do różnych platform

Dotychczas wiele firm nie przywiązywało wielkiej wagi do natychmiastowego cofnięcia pełnomocnictwa do PUE ZUS. Organ rentowy co jakiś czas apelował o uaktualnianie listy osób uprawnionych do dostępu do profilu, bo niektórzy płatnicy nie robili tego przez wiele lat. Jednak takie lekkie podejście do tej kwestii może się teraz zmienić, a wszystko za sprawą decyzji prezesa Urzędu Ochrony Danych Osobowych z 19 stycznia 2021 r., znak DKN.5131.33.2021 (opisywanej w DGP nr 36 z 22 lutego 2022 r. „O możliwym wycieku danych lepiej zawczasu poinformować"). Nałożył on na jeden z banków administracyjną karę pieniężną w wysokości ponad 545 tys. zł za niezawiadomienie bez zbędnej zwłoki o naruszeniu ochrony danych osób, których te dane dotyczą. Chodziło o to, że nie odebrano uprawnień dostępu do profilu na PUE ZUS byłemu pracownikowi, który, jak się w toku postępowania okazało, już po odejściu z firmy kilkakrotnie logował się do tego systemu. Karę nałożono, mimo że nie ustalono, czyje dokładnie dane były przeglądane ani czy były w jakikolwiek sposób później wykorzystane.

To ważna informacja nie tylko dla tych, którzy nie uaktualniają na bieżąco listy osób upoważnionych do profilu PUE ZUS. O decyzji UODO warto pamiętać także przy okazji dostępu do innych systemów z danymi np. klientów firmy.

Przynajmniej ostatniego dnia

Opisywana sprawa zaczęła się od samego banku, który poinformował UODO o naruszeniu danych osobowych po tym, jak wyszło na jaw, że były pracownik ciągle

posiada dostęp do profilu banku na PUE ZUS. Dzięki takiemu dostępowi można przeglądać dane osób zgłaszanych przez tego płatnika do ubezpieczeń, w tym m.in. imię, nazwisko, adres, PESEL. Płatnik (pracodawca) upoważnia osobę lub osoby do logowania się do jego profilu – może to być jego pracownik, ale także np. pracownik biura rachunkowego, które obsługuje firmę. W tym celu płatnik składa w ZUS odpowiednie pełnomocnictwo. Informacje dostępne na PUE są niezbędne, np. dla działu kadr czy księgowości, bo korzystając z nich, np. rozlicza się składki i świadczenia. Jeśli więc pracownik mający dostęp do firmowego profilu kończy pracę u danego pracodawcy, jego pełnomocnictwo powinno zostać cofnięte.

– Pracodawca powinien już tego samego dnia w prawidłowy sposób rozliczyć się z pracownikiem, zweryfikować, do jakich danych osobowych, kategorii oraz obszarów miał on dostęp. Konieczne jest także odwołanie nadanych upoważnień przez pracodawcę jako administratora danych osobowych, w tym odbiór przyznanych uprawnień i dostępów do systemów, w których znajdują się dane osobowe, karty wejść etc. – przypomina Monika Waraksa, aplikant adwokacki z kancelarii Wojarska Aleksiejuk i Wspólnicy. Agata Majewska, radca prawny z kancelarii Ślązak Zapiór i Partnerzy, zwraca uwagę, że czasami powinno to nastąpić nawet wcześniej. – Cofnięcie dostępu zwalnianego pracownika do danych zgromadzonych na PUE ZUS pracodawcy jako płatnika składek powinno nastąpić z momentem ustalenia, że nie jest on już niezbędny dla realizacji obowiązków przez danego zatrudnionego. Powinno nastąpić to nie tylko w razie definitywnego zakończenia współpracy, lecz także w razie przeniesienia na inne stanowisko, niezwiązane z obsługą PUE ZUS – wyjaśnia ekspertka. Cofnięcie dostępu do profilu może również okazać się uzasadnione, jeśli przed rozwiązaniem umowy o pracę pracownik korzysta z urlopu wypoczynkowego lub z innych powodów nie świadczy pracy. – W ten sposób pracodawca, działając jako administrator danych osobowych, powinien realizować zasadę minimalizacji danych i zgodności z celem przetwarzania – dodaje Agata Majewska.

Zawiadomienie bez zbędnej zwłoki

Prezes UODO uznał, że w tym przypadku doszło do naruszenia art. 34 ust. 1 RODO, tj. rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE z 2016 r. L 119, s. 1; ost.zm. Dz.Urz. UE 2021 r. L 74, s. 35). Zgodnie z tym przepisem, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to administrator bez zbędnej

zwłoki zawiadamia o tym osobę, której dane dotyczą. Z uzasadnienia wynika, że naruszenie poufności danych, jakie wystąpiło w sprawie w związku z naruszeniem ochrony danych osobowych polegającym na posiadaniu przez byłego pracownika dostępu do PUE ZUS, powoduje określone w tym przepisie „wysokie ryzyko naruszenia praw lub wolności osób fizycznych". W orzeczeniu podkreślono, że w sprawie nie jest istotne to, czy osoba nieuprawniona faktycznie zapoznała się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko (miała możliwość zapoznania się z tymi danymi). A jeśli się już z takimi danymi zapoznała, nie ma też znaczenia, czy dane w jakiś sposób wykorzystała (np. kopiując dane) czy nie. Prezes UODO podkreślił, że „dla powstania obowiązku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą, nie jest konieczne zmaterializowanie się negatywnych konsekwencji naruszenia, wystarczająca jest w tym zakresie sama możliwość (ryzyko) wystąpienia takich konsekwencji". Zdaniem regulatora bez znaczenia jest też to, że nie można stwierdzić, czyje dane były sprawdzane przez byłego pracownika. Jak czytamy w uzasadnieniu decyzji, „sam fakt braku precyzyjnie określonego kręgu pracowników, których naruszenie dotyczy, nie stanowi przeszkody dla realizacji obowiązku wynikającego z art. 34 rozporządzenia 2016/679 (RODO)". Formą takiego zawiadomienia może być komunikat publiczny, np. zamieszczony w Intranecie. Bank tego nie zrobił i została nałożona na niego kara.

Mniejsza skala naruszenia

Teoretycznie można więc wysnuć wniosek, że każde zaniedbanie firmy w odebraniu dostępu do PUE ZUS, i nie tylko (chodzi także o inne systemy z danymi zatrudnionych bądź klientów firmy), będzie naruszeniem ochrony danych osobowych. Jednak w przypadku banku były pracownik miał dostęp do PUE ZUS jeszcze kilka miesięcy po odejściu z pracy. Czy podobnie należałoby ocenić spóźnienie obejmujące np. zaledwie tydzień? Zdaniem ekspertów: tak. – Tygodniowe opóźnienie w oczywisty sposób może spowodować zarzut potencjalnego (a w istocie rzeczywistego) dostępu do danych pracowników przez osobę nieuprawnioną – mówi adwokat Marzena Kopij z kancelarii Kopij Zubrzycki. Także zdaniem Agaty Majewskiej taka zwłoka może powodować istotne ryzyko naruszenia bezpieczeństwa danych, a ryzyko to znacząco wzrasta w sytuacji, gdy pracodawca rozstaje się z pracownikiem w nieprzyjaznej atmosferze.

Nawet niewielka zwłoka może więc oznaczać naruszenie ochrony danych osobowych i jeśli tylko firma to odkryje, powinna o takim naruszeniu zawiadomić zainteresowanych. Z pewnością jednak prezes UODO, decydując o wymierzeniu ewentualnej kary lub jej wysokości, inaczej potraktowałby tego rodzaju przypadek niż

działanie banku w opisywanej sytuacji. Na wymiar kary wpłynęło bowiem nie tylko to, że byłemu pracownikowi nie odebrano dostępu do PUE przez długi czas, lecz także to, że bank podjął świadomą decyzję o rezygnacji z powiadomienia osób, których dane dotyczą, o zaistniałym naruszeniu. Bank argumentował bowiem, że ryzyko naruszenia praw lub wolności osób fizycznych nie było w tym przypadku wysokie, a zatem nie została spełniona przesłanka z art. 34 ust. 1 RODO.

Przeglądanie w trakcie pracy

Nieco inaczej sytuacja wygląda, gdy dane swoich kolegów bez powodu przegląda pracownik jeszcze w firmie zatrudniony i posiadający aktywny dostęp do PUE ZUS. W przeciwieństwie do tego już niepracującego może on bowiem ponieść konsekwencje pracownicze. Monika Waraksa zwraca uwagę, że pracodawca jako administrator powinien udzielić dostępu tylko do takich danych osobowych, które będą niezbędne do wykonywania czynności na zajmowanym stanowisku pracy, ograniczając tym samym dostęp do innych danych osobowych.

– Upoważnienie pracownika kadr do dostępu do PUE ZUS płatnika uprawnia do wykorzystywania zgromadzonych tam danych ubezpieczonych wyłącznie w celu prawidłowej realizacji obowiązków płatnika składek – podkreśla z kolei Agata Majewska. Jeśli przegląda on dane tylko dla własnej informacji, to jak wskazuje Marzena Kopij, będzie to stanowiło naruszenie obowiązków wynikających ze stosunku pracy, w szczególności wynikających z art. 100 kodeksu pracy. Może to stanowić ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować rozwiązaniem umowy o pracę bez wypowiedzenia z winy pracownika. Ekspertki podkreślają, że inne wykorzystanie danych z PUE ZUS stanowiłoby ich przetwarzanie niezgodnie z zakresem i celem upoważnienia, co skutkować może odpowiedzialnością porządkową, ale również materialną pracownika – jeśli pracodawca lub osoba trzecia ponieśliby z tego tytułu szkodę.

W tego rodzaju sprawach trudno jest jednak udowodnić, że pracownik przeglądał dane swoich kolegów bez powodu, bo w przeciwieństwie do sytuacji będącej przedmiotem opisywanej decyzji, w tym przypadku pracownik dostęp powinien posiadać, a nieprawidłowe jest jego użycie. W praktyce tego rodzaju spory będą więc należały do rzadkości. ©℗

MP MONITOR
prawa pracy i ubezpieczeń

Autor
Joanna Śliwińska
joanna.sliwinska@infor.pl